(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 May 2005 (06.05.2005)

PCT

(10) International Publication Number
WO 2005/041185 A1

(51) International Patent Classification: G11B 20/00

(21) International Application Number:
PCT/EP2004/009393

(22) International Filing Date: 23 August 2004 (23.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03090341.3 13 October 2003 (13.10.2003) EP

(71) Applicant *(for all designated States except US)*: **THOMSON LICENSING S.A.** [FR/FR]; 46 Quai A. Le Gallo, F-92100 Boulogne-Billancourt (FR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ADOLPH, Dirk** [DE/DE]; Wallbrink 2, 30952 Ronnenberg (DE). **HÖRENTRUP, Jobst** [DE/DE]; Gabelsbergerstr. 18, 30163 Hannover (DE). **JANSSEN, Uwe** [DE/DE]; Niedersachsenstr. 53, 30926 Seelze (DE). **OSTERMANN, Ralf** [DE/DE]; Oberstr. 17, 30167 Hannover (DE). **HERPEL, Carsten** [DE/DE]; Grosse Barlinge 61, 30171 Hannover (DE).

(74) Agent: **RITTNER, Karsten**; Deutsche Thomson-Brandt GmbH, European Patent Operations, Karl-Wiechert-Allee 74, 30625 Hannover (DE).

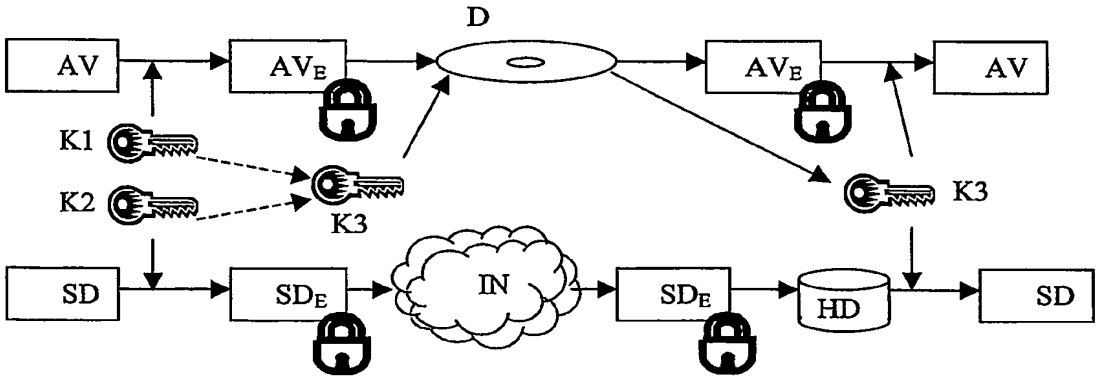
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR DECRYPTING AN ENCRYPTED SUPPLEMENTARY DATA SET



(57) Abstract: Removable media such as optical discs (D) may carry valuable audio-visual data representing movies or the like, which are sold by content providers or studios. To prevent pirate copies, data (AV_E) on these media are often encrypted for copy protection. This copy protection may use a disc specific electronic decryption key (K3), which is stored on the disc itself. Supplementary data (SD) such as games, subtitle or audio streams that are regarded as being closely related to disc contents, but are not stored on the disc itself, are encrypted so that decryption is only possible with a decryption key (K3) retrieved from the disc (D), or in particular the same decryption key that is used for the disc contents (AV_E). The method is particularly effective for copy protection or cross usage exclusion of supplementary data (SD_E) when the decryption key (K3) is prevented from being accessible to the user.

WO 2005/041185 A1